



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 150  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/084,499	02/28/2002	Zhichen Xu	100200290-1	7480

7590 08/02/2006

HEWLETT-PACKARD COMPANY  
Intellectual Property Administration  
P.O. Box 272400  
Fort Collins, CO 80527-2400

EXAMINER

WILLIAMS, JEFFERY L

ART UNIT	PAPER NUMBER
----------	--------------

2137

DATE MAILED: 08/02/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

Application No.

10/084,499

Applicant(s)

XU ET AL.

Examiner

Jeffery Williams

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 06 September 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1,3-12,14-25 and 27-44 is/are pending in the application.
- 4a) Of the above claim(s) 31-41 is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1,3-12,14-25,27-30 and 42-44 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 08 February 2002 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- ☒ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- ☐ Notice of Informal Patent Application (PTO-152)
- ☐ Other: \_\_\_\_\_

**DETAILED ACTION**

This action is in response to the communication filed on 6/6/06.

All objections and rejections not set forth below have been withdrawn.

Claims 1, 3 – 12, 14 – 25, 27 – 30, and 42 – 44 are pending.

***Specification***

The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required:

Claim 42 recites the limitations "*if **a label** stored at an intermediate peer of the plurality of peers does not match the predetermined label in the set-up message, the intermediate peer stores the predetermined label and the corresponding identity of the next peer*" [emphasis added]. The specification does not provide antecedent basis for storing the predetermined label upon condition that **a label** does not match.

Claim 44 recites the limitation, "*wherein the stored message comprises: an encryption key encrypted with the public key of the requestor*". This limitation is not supported in the specification.

***Claim Rejections - 35 USC § 112***

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 42 – 44 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. See above objection to the specification.

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

**Claims 1, 8 – 12, 20 – 25, 27 – 30, and 42 – 44 are rejected under 35 U.S.C. 102(b) as being anticipated by Goldschlag et al. (Goldschlag), “Hiding Routing Information”.**

Regarding claim 1, Goldschlag discloses:

*forming a path from a provider to a requestor by selecting a plurality of peers in response to receiving a request for information (Goldschlag; page 2, par. 2 – page 3; page 4, par. 3)*

*updating a table on each peer of said plurality of peers with a respective path index entry for said information (Goldschlag, page 10, par. 4, lines 14-18);*

*transmitting a message to said requestor through said plurality of peers, said message comprising said information and a path index for said information from said provider; and determining a next peer according to said path for said information by searching said table of each peer of said plurality of peers with said path index as an index into said table (Goldschlag, page 11, par. 2);*

*retrieving an identity of said next peer according to said path for said information and a respective index peer of said next peer; encrypting said path index with a public key of said respective index peer of said next peer to form a next state of said path index; and transmitting a new message with said information and said next state of said path index as said path index to said next peer (Goldschlag, page 11; fig. 2; page 5).*

Herein, Goldschlag discloses that a node utilizes information to retrieve the identity of the next peer in the path, and thus retrieves the identity of the next peer “according to the path ... and a respective index peer” of the next peer, encrypts with the public key of the next peer, thus forming “a next state of path index”, and sends the message.

Regarding claim 8, Goldschlag discloses:

1        *forming a respective path message to each peer of said plurality of peers, said*  
2        *respective path message comprising said respective path index entry (Goldschlag, page*  
3        *10, par. 4).*

4  
5        Regarding claim 9, Goldschlag discloses:

6        *The method according to claim 8, wherein said respective path index entry*  
7        *comprises an identity of a next peer according to said path, a respective index peer for*  
8        *said next peer, and an index entry (Goldschlag, page 6, par. 1; page 10, par. 4).*

9  
10       Regarding claim 10, Goldschlag discloses:

11       *wherein said identity of next peer according to said path and said respective*  
12       *index peer for said next peer are encrypted with a public key of a peer receiving said*  
13       *respective path message (Goldschlag, page 6, par. 1; page 10, par. 4).*

14  
15       Regarding claim 11, Goldschlag discloses:

16       *wherein said index entry is formed according to [public.sub.b.sub..sub.j1( . . .*  
17       *public.sub.b.sub..sub.j1(public.sub.b.sub..sub.j0(n)) . . . )], where b.sub.j represents said*  
18       *respective index peer (Goldschlag, fig. 2; page 5, line 2; fig. 4).*

19  
20       Regarding claim 12, it is rejected, at least, for the same reasons as claim 1, and  
21       furthermore because Goldschlag discloses:

1        *updating a respective table of each peer of a plurality of peers with a respective*  
2        *path index entry in response to receiving a path formation message containing said*  
3        *respective path index entry (Goldschlag; page 2, par. 2 – page 3; page 4, par. 3; page*  
4        *10, par. 4, lines 14-18);*

5        *receiving a message comprising said information and a path index; and*  
6        *forwarding said information to a next peer in response to a determination of said next*  
7        *peer from said table with said path index as a search index into said table (Goldschlag,*  
8        *page 11, par. 2).*

9  
10        Regarding claim 20, Goldschlag discloses:

11        *receiving said message at said requestor; applying a complementary key to said*  
12        *public key of said requestor to said encryption key encrypted with said public key of said*  
13        *requestor to obtain said encryption key; applying said encryption key to said encrypted*  
14        *reference to retrieve said information (Goldschlag, page 6, par. 2; page 11, par. 2).*

15  
16        Regarding claim 21, Goldschlag discloses:

17        *selecting a path for information from a provider to a requestor through a plurality*  
18        *of peers in response to a received request for said information (Goldschlag, page 6, par.*  
19        *1); receiving a respective set-up message at each peer of said plurality of peers,*  
20        *wherein said respective set-up message comprises a predetermined label and an*  
21        *identity of a next peer for said information according to said path (Goldschlag, page 6,*  
22        *par. 1).*

1           *generating an encryption key; encrypting said encryption key with a public key of*  
2           *said requestor; encrypting said encryption key with a public key of said provider*  
3           (Goldschlag, page 5); *and encrypting a transaction identifier, a reference for said*  
4           *information, and a first next peer according to said path with said encryption key*  
5           (Goldschlag, page 5, line 2; page 6, par. 1; page 8, par. 1; page 11, pars. 1, 2). Herein,  
6           Goldschlag discloses the encryption with an encryption key *a reference for said*  
7           *information* (such as, payload – pg. 5, line 2), *a transaction identifier* (such as,  
8           exp\_time<sub>y</sub> – a transaction identifier identifying a transferred onion Y and identifying a  
9           validity period for said transferred onion Y), *and a first next peer according to said path*  
10          (i.e. “Z” – a next peer).

11  
12          Regarding claim 22, it is rejected, at least, for the same reasons as claim 1.

13  
14          Regarding claim 23, Goldschlag discloses:

15          *receiving a message, wherein said message comprises: an encryption key*  
16          *encrypted with a public key of said requestor; said information encrypted with said*  
17          *encryption key; and a message label; and retrieving said identity of next peer from said*  
18          *table in response to said message label matching said predetermined label in said table*  
19          (Goldschlag, page 8, par. 1; page 11, par. 2).

20  
21          Regarding claim 24, it is rejected, at least, for the same reasons as claim 2.

22



1           Regarding claim 25, Goldschlag discloses:

2           *comparing said identity of said next peer with a current peer; decrypting said*  
3 *encryption key encrypted with a public key of said requestor in response to said identity*  
4 *of said next peer being said current peer; and decrypting said information encrypted*  
5 *with said encryption key (Goldschlag, page 11, pars. 1,2).*

6  
7           Regarding claim 27, Goldschlag discloses:

8           *forming a retrieval message comprising: said encryption key encrypted with said*  
9 *public key of said requestor; said encryption key encrypted with said public key of said*  
10 *provider; said transaction identifier, said reference for said information, and said first*  
11 *next peer according to said path encrypted with said encryption key; and transmitting*  
12 *said retrieval message to said provider (Goldschlag, pages 4, 5; page 6, pars. 1,2; page*  
13 *8, par. 1; page 11, pars. 1, 2).*

14  
15           Regarding claim 28, Goldschlag discloses:

16           *applying a complementary key of said provider to said encryption key encrypted*  
17 *with said public key of said provider; and decrypting said reference for said information,*  
18 *said transaction identifier, and said first next peer (Goldschlag, page 6, pars. 1, 2).*

19  
20           Regarding claim 29, Goldschlag discloses:

21           *retrieving said information based on said reference for said information;*  
22 *encrypting said information with said encryption key; and forming a message label*

1 *based on said transaction identifier* (Goldschlag; page 2, par. 2 – page 3; page 4, par. 3;  
2 *page 8, par. 1; page 10, par. 4; page 11, pars. 1,2).*

3  
4       Regarding claim 30, Goldschlag discloses:  
5       *forming a message including said encrypted information and said message label;*  
6 *and transmitting said message to said first next peer* (Goldschlag, page 11, pars. 1,2).

7  
8       Regarding claim 42, it is rejected, at least, for the same reasons as claims 2, 13,  
9 and 22, and furthermore because Goldschlag discloses:

10       *if a label stored at an intermediate peer of the plurality of peers does not match*  
11 *the predetermined label in the set-up message, the intermediate peer stores the*  
12 *predetermined label and the corresponding identity of the next peer* (Goldschlag, page  
13 5, par 1). Herein Goldschlag discloses that the intermediate peer stores received  
14 messages. A message comprises the label and identity of the next peer. Such is the  
15 operation disclosed by Goldschlag and is what will occur *if a label stored at an*  
16 *intermediate peer of the plurality of peers does not match the predetermined label in the*  
17 *set-up message.*

18       *if a label stored at the intermediate peer matches the predetermined label, the*  
19 *intermediate peer retrieves a previously stored message and generates a next state of*  
20 *the predetermined label for the setup message* (Goldschlag, page 5, par 1; page 6, par.  
21 1, lines 8-18). Herein, Goldschlag discloses that the peer stores “a message” which is  
22 retrieved and later utilized for the sending of messages. Goldschlag further discloses

1 that the peer also formats a message utilizing the appropriate data necessary for  
2 transmission to the next peer ["generates a next state of the predetermined label"].  
3 Such is the operation disclosed by Goldschlag and is what will occur *if a label stored at*  
4 *the intermediate peer matches the predetermined label.*

5  
6 Regarding claim 43, Goldschlag discloses:  
7 *encrypting the received predetermined label with a public key of a respective*  
8 *index peer of the next peer* (Goldschlag, page 5).

9  
10 Regarding claim 44, Goldschlag discloses:  
11 *an encryption key encrypted with the public key of the requester* (Goldschlag, fig.  
12 2; page 5).

13  
14  
15 ***Claim Rejections - 35 USC § 103***

16  
17 The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all  
18 obviousness rejections set forth in this Office action:

19 (a) A patent may not be obtained though the invention is not identically disclosed or described as set  
20 forth in section 102 of this title, if the differences between the subject matter sought to be patented and  
21 the prior art are such that the subject matter as a whole would have been obvious at the time the  
22 invention was made to a person having ordinary skill in the art to which said subject matter pertains.  
23 Patentability shall not be negated by the manner in which the invention was made.  
24

1           **Claims 3 – 7 and 14 – 19 are rejected under 35 U.S.C. 103(a) as being**  
2           **unpatentable over Goldschlag in view of Clarke et al. (Clarke), “Freenet: A**  
3           **Distributed Anonymous Information Storage and Retrieval System”.**  
4

5           Regarding claim 3, Goldschlag discloses a system for requesting and retrieving  
6           information on a network. The system employs a method for hiding the path (creating  
7           an anonymous connection) for such requests and replies (Goldschlag, pages 1-3).  
8           Goldschlag discloses the receiving of a request for information, and the formation of a  
9           path to said requested information (see rejection of claim 1). Goldschlag, however,  
10          does not disclose that the reception for a request for information was at a directory, a  
11          determination of availability, or a notification of non-availability.

12          Clarke similarly discloses a system for requesting and retrieving information,  
13          anonymously, on a network. More specifically, Clarke discloses methods for requesting  
14          and receiving information, where the information consists of file transactions (Clarke,  
15          page 2, par. 1). Because onion routing systems, such as disclosed by Goldschlag, do  
16          not focus on the publication, access, and storage of files, Clarke discloses that this  
17          system is “best viewed as a complement” to such a onion routing system. Clarke  
18          discloses that an additional advantage of such a combination is increased security  
19          (Clarke, page 17, table 1, pars. 1-4).

20          It would have been obvious to one of ordinary skill in the art to employ the  
21          methods of Clarke within the system of Goldschlag. This would have been obvious

1 because one of ordinary skill in the art would have known the explicit teachings for the  
2 combination of these systems, as well as recognized the benefits of additional security.

3 Thus, the combination of Goldschlag and Clarke disclose:

4 *receiving said request for information at a directory* (Clarke, page 3, par. 3, lines  
5 1-6; page 18, lines 2-6; page 18, par. 2; page 4, pars. 1, 2). Clark discloses that each  
6 node acts as a directory containing the locations to requested files.

7 *determining an availability of said information* (Clarke, page 6, par. 4);

8 *and notifying said requestor of a determination of non-availability* (Clarke, page 6,  
9 par. 4). The combination of Goldschlag and Clarke discloses that the method includes  
10 notifying the requestor of a decision ("determination") of the quality or state of being  
11 non-available ("non-availability") of the requested file. In this case, if the file is available,  
12 the method notifies the requester that the file is available - a decision of non-affirmation  
13 regarding the quality of the file being non-available. Furthermore, the combination of  
14 Goldschlag and Clarke discloses that the method includes notifying a requester that it  
15 has been determined that a file is not available on a particular node (Clarke, page 6,  
16 par. 5, lines 3,4).

17  
18 Regarding claim 4, the combination of Goldschlag and Clarke disclose:

19 *receiving said request for information at a directory* (Clarke, page 3, par. 3, lines  
20 1-6; page 18, lines 2-6; page 18, par. 2; page 4, pars. 1, 2). The combination of  
21 Goldschlag and Clarke discloses that each node acts as a directory containing the  
22 locations to requested files.

1           *determining an availability of said information* (Clarke, page 6, par. 4);  
2           *and generating an encryption key in response to a determination of said*  
3           *availability* (Clarke, page 3, par. 3, lines 1-6; page 18, lines 2-6; page 18, par. 2; page 4,  
4           pars. 1, 2). The combination of Goldschlag and Clarke discloses that when a file is  
5           found to be available on a remote node, the request for the file is forwarded to the  
6           remote node. When such requests are forwarded, the combination of Goldschlag and  
7           Clarke discloses that these requests are link encrypted with an encryption key. The  
8           process of encrypting a request with an encryption key clearly results in the process of  
9           coming into being (the "generation") of an encryption key, whether the key is produced  
10          from storage, received over a network, or the resultant of a key-derivation algorithm  
11          (Goldschlag, fig. 1; page 10, par. 3).

12  
13          Regarding claim 5, the combination of Goldschlag and Clarke disclose:  
14          *determining a first next peer from said provider and a respective index peer for*  
15          *said first next peer according to said path; and encrypting a reference to said*  
16          *information, said first next peer, and said respective index peer of said first next peer*  
17          *with said encryption key* (Goldschlag, page 6, par. 1).

18  
19          Regarding claim 6, the combination of Goldschlag and Clarke disclose:  
20          *wherein said encryption key is generated according to a DES encryption*  
21          *algorithm*. Goldschlag discloses using a efficient symmetric algorithm for the encryption  
22          key, however, Goldschlag does not specify DES encryption. It would have been

1 obvious to use DES encryption as this is an efficient algorithm used in the onion routing  
2 system as evidenced by Goldschlag, "Anonymous Connections and Onion Routing",  
3 page 6, section E – Onions).

4  
5 Regarding claim 7, the combination of Goldschlag and Clarke disclose:  
6 *encrypting said encryption key with a public key of said requestor; encrypting*  
7 *said encryption key with a public key of said provider; forming a provider message,*  
8 *wherein said provider message comprises: said encryption key encrypted with said*  
9 *public key of said requestor; said encryption key encrypted with said public key of said*  
10 *provider; said encrypted reference; and said encrypted first next peer and said*  
11 *respective first index peer; and transmitting said message to said provider* (Goldschlag,  
12 page 6, section 3.1).

13  
14 Regarding claim 14, it is rejected, at least, for the same reasons as claim 3.

15  
16 Regarding claim 15, it is rejected, at least, for the same reasons as claims 4 and  
17 5.

18  
19 Regarding claim 16, it is rejected, at least, for the same reasons as claims 4 – 7.

20  
21 Regarding claim 17, it is rejected, at least, for the same reasons as claim 6.

22

Regarding claim 18, the combination of Goldschlag and Clarke disclose:

*receiving said second message at said provider; applying a complementary key to said public key of said provider to said obtain said encryption key; and applying said encryption key to said encrypted reference to retrieve said reference* (Goldschlag, page 6, section 3.1).

Regarding claim 19, it is rejected, at least, for the same reasons as claim 7, and furthermore because the combination of Goldschlag and Clarke disclose the retrieving of information based upon a reference (a request for said information) (Clarke, section 3.2).

### ***Response to Arguments***

Applicant's arguments filed 6/6/06 have been fully considered but they are not persuasive.

Applicant's argue primarily that:

(i) *Goldschlag fails to teach an index peer of a next peer, retrieving an identity of a next peer using a respective index peer of the next peer, and encrypting the path index with public key of the index peer of the next peer.* (Remarks, pg. 13)



1

2           In response to applicant's argument that the references fail to show certain  
3 features of applicant's invention, it is noted that the features upon which applicant relies  
4 (*i.e., retrieving an identity of a next peer using a respective index peer of the next peer*)  
5 are not recited in the rejected claim(s). Although the claims are interpreted in light of  
6 the specification, limitations from the specification are not read into the claims. See *In*  
7 *re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

8           Furthermore, as pointed out in the above rejected claims, the examiner  
9 respectfully notes that Goldschlag discloses utilizing identity information to retrieve the  
10 identity of the next peer and encrypting the message with the public key associated with  
11 the identity information. Thus Goldschlag teaches *an index peer of a next peer* and  
12 *encrypting the path index with public key of the index peer of the next peer*.

13

14 (ii)   Thus, Goldschlag discloses *encrypting payload data of the data stream with the*  
15 *function key pairs. However, the virtual circuit identifier in Goldschlag is not encrypted*  
16 *with the function key pairs or a public key of an index peer of a next peer. Accordingly,*  
17 *claims 1 and 3-11 are believed to be allowable.* (Remarks, pg. 14)

18

19           Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount  
20 to a general allegation that the claims define a patentable invention without specifically  
21 pointing out how the language of the claims patentably distinguishes them from the  
22 references.

1       Applicant's arguments do not comply with 37 CFR 1.111(c) because they do not  
2       clearly point out the patentable novelty which he or she thinks the claims present in view  
3       of the state of the art disclosed by the references cited or the objections made. Further,  
4       they do not show how the amendments avoid such references or objections.

5  
6       (iii)     *Also, claim 11 is directed to an index entry including respective index peers,*  
7       *which is not taught by Goldschlag.*

8  
9       In response, as pointed out in the rejection of claim 11, the examiner respectfully  
10      asserts that Goldschlag discloses wherein a message is formed according to the  
11      claimed manner.

12             Furthermore, the examiner points out that *an index entry including*  
13      *respective index peers* is not recited in the claim language. In response to applicant's  
14      argument that the references fail to show certain features of applicant's invention, it is  
15      noted that the features upon which applicant relies (i.e., *index entry including respective*  
16      *index peers*) are not recited in the rejected claim(s). Although the claims are interpreted  
17      in light of the specification, limitations from the specification are not read into the claims.  
18      See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

19  
20  
21      (iv)     *Goldschlag fails to teach this feature for the reasons stated above.* (Remarks,  
22      pg. 15 – regarding rejection of claim 12)

1  
2 In response, the examiner finds the applicant's arguments to be unpersuasive in  
3 light of the reasons made of record.

4  
5 (v) *However, Goldschlag fails to teach the two function key pairs are used to encrypt*  
6 *a transaction identifier, a reference for said information, and a first next peer according*  
7 *to said path with said encryption key. (Remarks, pg. 15)*

8  
9 In response, the examiner finds the applicant's arguments to be unpersuasive in  
10 light of the reasons made of record. As stated in the rejection of claim 21, an encryption  
11 key is used to encrypt *a transaction identifier, a reference for said information, and a*  
12 *first next peer according to said path.*

13  
14 (vi) Applicant argues the added limitations to the amended claim 42. (Remarks, pg.  
15 16)

16  
17 In response, the examiner respectfully directs the applicant's attention to the  
18 rejection of claim 42.

19  
20 (vii) *Neither Clarke nor Goldschlag discloses a peer similar to the directory 130.*  
21 *Thus, there is unreasonable expectation of success when combining the onion routing*

1 *of Goldschlag with Clarke. Accordingly, a prima facie case of obviousness has not*  
2 *been established and the rejection should be withdrawn. (Remarks, pg. 17)*

3  
4 In response the examiner respectfully directs the examiners attention to the prior  
5 art references and the appropriate rejections. Therein, suggestion for the combination  
6 is shown, and accordingly an expectation of success is seen.

7 In response to applicant's argument that the references fail to show certain  
8 features of applicant's invention, it is noted that the features upon which applicant relies  
9 (i.e., *a peer similar to the directory 130*) are not recited in the rejected claim(s).

10 Although the claims are interpreted in light of the specification, limitations from the  
11 specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26  
12 USPQ2d 1057 (Fed. Cir. 1993).

13 Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount  
14 to a general allegation that the claims define a patentable invention without specifically  
15 pointing out how the language of the claims patentably distinguishes them from the  
16 references.

17 Applicant's arguments do not comply with 37 CFR 1.111(c) because they do not  
18 clearly point out the patentable novelty which he or she thinks the claims present in view  
19 of the state of the art disclosed by the references cited or the objections made. Further,  
20 they do not show how the amendments avoid such references or objections.

21  
22 (viii) Applicant points out the addition of new claims 43 and 44. (Remarks, pg. 17)

1  
2 In response, the examiner respectfully directs the applicant's attention to the  
3 rejections of claims 43 and 44.

4  
5  
6 ***Conclusion***

7  
8 The prior art made of record and not relied upon is considered pertinent to  
9 applicant's disclosure.

10 *See Notice of References Cited.*

11  
12 **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time  
13 policy as set forth in 37 CFR 1.136(a).

14 A shortened statutory period for reply to this final action is set to expire THREE  
15 MONTHS from the mailing date of this action. In the event a first reply is filed within  
16 TWO MONTHS of the mailing date of this final action and the advisory action is not  
17 mailed until after the end of the THREE-MONTH shortened statutory period, then the  
18 shortened statutory period will expire on the date the advisory action is mailed, and any  
19 extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of  
20 the advisory action. In no event, however, will the statutory period for reply expire later  
21 than SIX MONTHS from the mailing date of this final action.

Art Unit: 2137

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffery Williams whose telephone number is (571) 272-7965. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

J. Williams  
AU: 2137

  
EMMANUEL L. MOISE  
SUPERVISORY PATENT EXAMINER

JW